The Future Internet: The Social Nature of Technical Choices
A SEMINAR ORGANIZED BY SESERV

Cross-thematic trends of break-out sessions

1.1. Call for increased transparency (systems and data use)

A dominant trend across discussions in all six break-out sessions, is a call for increased transparency on all levels for end-users of networked ICTs. Systems and applications should offer end-users tools that allow for filtering of information and sharing of content in order to ensure that end-users know exactly who has access to, for example, their online social network content. Advanced transparent filtering options are becoming increasingly important as more and more online networks are being synchronized, thus creating an even greater need for tools that can assist users in managing their online communities.

Transparency also relates to ISPs and data storage, particularly with the move towards more cloud-based services. Many companies for example run services on 3rd parties' infrastructure, which is not sufficiently transparent to end-users. To make security risks more transparent for end-users, providers could e.g. publish monthly statistics on attacks. End-users should also be able to easily identify where and how their data is stored. How data is used/will be used could also be disclosed.

1.2. Call for more user-centricity and control

All six break-out sessions to some extend expressed a call for more user-centricity and control. A prominent theme here was the need for increased user-centricity in the design of applications. In extension to this, users could be allowed means of influencing applications/systems on an ongoing basis; creative uses could feed back into systems to improve and innovate them.

A common argument put forward is the latent scope for much more user control. Control is particularly addressed in the context of opt-out options: users should be able, in a more granular manner, to opt out of services or elements of services. Additionally, a range of different choices for how users' data is stored could be offered (e.g. servers' geographical location). Finally, users should have better ways of assessing and controlling their security risks and risk management.

1.3. Continuing need for further multi-disciplinary bridging

Without exceptions the break-out discussions address the need for further multi-disciplinary bridging. This trend unambiguously calls for knowledge-exchange, dialogue and collaboration across and beyond academic fields, industry, developers, designers and users. Several of the discussions addressed existing gaps, for example, between privacy researchers and IoT engineers, and between eHealth practitioners and IT suppliers.

Potential ways of ensuring further multi-disciplinary bridging are initiating frameworks for knowledge exchange between users, developers, regulators and researchers. Other ways to avoid silozation is facilitating connections between technical and legal analysts to develop a better understanding of risks. It is important to acknowledge different communities' expertise, and bring a range of diverse human resources into all, including early, stages of technology development and design. There is a need for examining the frequency of multi-disciplinary conferences, and possibly fund larger numbers of multi-disciplinary research centres.

1.4. Addressed need for striking balances between outer-poles in debates and design

A meta cross-theme that emerged from 4 break-out discussions (identity; online communities; IoT; privacy) was a call for more balanced approaches in discussions and in design, avoiding dichotomies and outer-pole positions. For identity discussions, for example, it was argued that there is a need to balance viewpoints of identity as either singular and stable (e.g. passport) or multiplex and absolute dynamic. How identity is perceived and defined bears consequences for system design, and more nuanced views and further multi-disciplinary research are arguably needed. It is important to allow for understandings and discussions of identity that acknowledge it as existing on a continuum ranging from stable to dynamic.

With respect to design, there is a need for more balanced approaches including both bottom-up and bottom-down innovation. It is for example possible that new forms of communities or structures might emerge in the social world, and that these are potential drivers of technology development.

Other balances to strike can be exemplified through eHealth privacy practices and discussions. As far as e.g. patient records goes, it might be beneficial to seek a middle solution that allows proportionate access, rather than relying on either lassez-faire approaches or access over-formalisation (extreme regulation) as is arguably currently the case.

Discourses on privacy issues tend to lack balance. It is necessary to balance privacy concerns with the affordances of given technologies; in particular Internet of Things technologies, that are often perceived as 'big brother' enforcement.

1.5. Need for facilitating further digital literacy development

Directly and indirectly the need for providing more digital and media literacy education was addressed in the sessions on Security, Privacy, Identity and Online Communities. The core concerns related to users' ability to critically manage privacy and identity concerns. Arguably, digital literacy skills can equip users with more sophisticated tools for managing and understanding identity in online and hybrid contexts, and might solve some of the problems that emerges from privacy concerns. Security risks could be better understood if best practice guidelines were available, and more awareness was raised. This theme points to some of the non-technical social barriers and challenges that need to be addressed alongside the design and development of socio-technical systems of the future internet.

1.6. Addressing lack of common vocabularies and definitions

Several of the break-out sessions address an explicit need for developments of common vocabularies and better definitions (Identity; IoT; Online Communities; Cloud Computing). In cloud computing, for example, current definitions are diverging: some refer exclusively to infrastructure, while others include social uses and online activities. For definitions of Internet of Things the problem is that they currently are too academic, lack focus on design, and therefore are difficult to apply in technology development. For identity, there is a need for definitions that acknowledges that identity is closely related to questions of privacy, data and rights in digital contexts.

The emergence of new technologies, and new uses, require the development of vocabularies enabling discussions on such interactions/technologies. At present, there are no applicable vocabularies for describing multi-device Internet of Things interactions. Likewise, it seems that there is a need for more advanced vocabulary to describe online communities' and networks' health (e.g. related to growth, maintainable, structure, size).

Seen in the light of the pronounced call for multi-disciplinary bridging and collaboration, it seems urgent to take action on initiatives that can help facilitate the development of adequate vocabulary and definitions that can be applied across sectors/contexts.

1.7. Need for clarifying digital rights (including digital choice)

The discussions facilitated in the break-out sessions on Privacy, Internet of Things and on Online Communities addressed issues that relates to the need for clarifying digital rights and digital choices. One of the central questions raised here was which levels of anonymity should be granted; and to whom and in which contexts. In eHealth, for example, one of the challenges is to balance the individual's right to anonymity, while still ensuring access to enough identifiers so that emerging health issues can be detected.

Another central issue addressed, was to which extend digital rights should include the right to be forgotten; to have information deleted. In the discussion, it was suggested that this right might not apply to information in the pubic sphere, and that there might be content that had too historic or humanitarian value. An example could be holocaust-related information.

Digital choice formed part of the discussions. For Internet of Things technologies, it was underlined that off-line alternatives should be available. Digital choice relates to the right to not make use of technologies, without being penalized.

1.8. Inviting global regulatory frameworks

The final cross-theme emerging from the break-out sessions has to do with a call for more global regulatory frameworks. In discussions on Security, Online Communities and Cloud Computing, this need was addressed. Some of the areas that were suggested focused on consistency in laws across jurisdictions for data breach and notification, and anonymity (conditional / dependent on domain, e.g. politically sensitive topics). Increased transnational legislation could also ensure that providers are not discouraged from operating in certain countries (for example if this country holds providers liable for IP infringement by users).

Authors: Isis Hjorth, Bianca Reisdorf, Chrysanthi Papoutsi, Lucy Power, Nesrine Abdel-Sattar and Scott Hale (Oxford Internet Institute, University of Oxford).

http://www.seserv.org